APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/567,662	02/08/2006	Amnon Yacoby	ANI-002-NP	3988

24964   7590   06/19/2009

GOODWIN PROCTER LLP
ATTN: PATENT ADMINISTRATOR
620 Eighth Avenue
NEW YORK, NY 10018

EXAMINER
CHRISTENSEN, SCOTT B

ART UNIT	PAPER NUMBER
2444	

MAIL DATE	DELIVERY MODE
06/19/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *19 February 2009*.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *26-45* is/are pending in the application.
  4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) *26-45* is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  a) ☐ All b) ☐ Some * c) ☐ None of:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. _____.
    3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
  Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   This Office Action is in regards to the most recent papers filed on 2/19/2009.

Response to Arguments

2.   Applicant's arguments filed 2/19/2009 have been fully considered but they are
not persuasive.

3.   On pages 5-6 of Applicant's arguments, Applicant argues the rejection of claim
26. More specifically, Applicant argues that "a system where a proxy (agent) is
deployed onto a network element and is used to perform the operations of a
configuration plan to change the settings of a network element" is substantially different
from "selecting a policy to be implemented by at least one second network element,
different from the first network element, responsive to the collected real time information
from the one or more first network elements, the at least one second element including
an end-point element of the network, and enforcing the selected policy on the agent
hosted by the at least one second network element.." Applicant argues that this is the
case as "unlike the e-Security and Mattila systems, the proposed system performs real-
time selection of an enforceable policy in response to real-time operational input data
collected from the one set of network elements and implementation of this policy on
another set of network elements."

        First, it is noted that the instant claim does not include any language that
suggests that the proposed system performs "real-time" selection. Rather, the instant

method simply selects a policy to be implemented responsive to real-time information that was collected in the first step.

Meanwhile, Mattila discloses utilizing a configuration plan to change settings of a network element. A network administrator who receives the information from e-Security could utilize a system such as that of Mattila to make configuration changes to change the settings to address the issues that arose from the e-Security system. The instant claim provides for no requirement as to what entity actually performs the selecting, only that it occurs. In this case, the proposed combination, even when performed manually by a network administrator, is similar in scope to the instant claim.

Applicant should amend the claim to clearly state what entity is performing the functionality, and how the selection of the policy is related to the collected information in more detail than simply "responsive."

4.   On pages 6-7, Applicant argues the rejection of claim 27. More specifically, Applicant argues that e-Security as modified by Mattila does not teach "information on operation problems."

However, the instant claim provides no detail on what "operation problems" is limited to. The security events of e-Security entail operation problems, as a security problem is also a problem with the operation of a device.

Applicant should amend the claim to clearly recite what is meant by "operation problems."

5.   On pages 7-8, Applicant argues the rejection of claim 28. More specifically,

Applicant argues that e-Security does not teach collecting information on software

applications installed or running on network elements.

However, the instant claim provides absolutely no detail on what information on

software applications installed or running on network elements is collected. In the case

of e-Security, at least the operating systems are monitored. The claimed term "software

application" is interpreted as including any software application, where in the case of the

claim, the software application must be installed or running on network elements. Thus,

an operating system is within the scope of a software application.

If Applicant intends for "software applications" to have a specific meaning,

Applicant should amend the instant claim to clearly limit "software applications" to the

intended scope.

6.   On pages 8-9, Applicant argues the rejection of claim 29. More specifically,

Applicant argues that the detection of application crashes and system crashes is

substantially different.

However, in determining the scope of a claim, the claim must be given the

broadest reasonable interpretation from the perspective person of ordinary skill in the

art. Thus, a system crash is not limited to the catastrophic system crash that results in

the entire system being inoperable. Rather, a system crash is interpreted as being any

crash that pertains to the system, which includes both complete crashes and partial

crashes (e.g. only a part of the system crashes).

If Applicant intends for a system crash to be where the entire device is

inoperable, the instant claims should be amended to reflect this.

7.   On page 10, Applicant argues the rejection of claim 30. More specifically,

Applicant argues that "operating systems and antivirus software" is substantially

different from "generic collection of any software installed and used on the host."

However, in rejecting a claim, the scope of the claim is first determined. Then, if

prior art is found that teaches any embodiment within the scope of the claim, then the

claim is properly rejected utilizing that prior art. In this case, the claim refers to

"software applications." Thus, any software application disclosed is enough to satisfy

the claim language, whether the software application is generic or specific. Accordingly,

even though e-Security teaches specific examples, the claim is still properly rejected as

the specific examples are still "software applications."

8.   On pages 10-11, Applicant argues the rejection of claim 31. More specifically,

applicant broadly asserts that the teachings of e-Security are "substantially different"

from "monitoring of each communication path."

However, the instant claim provides no requirement to monitor any

communication path, only to monitor communications between network elements.

Accordingly, this can be performed by monitoring communication paths, as proposed by

Applicant, or monitoring the devices that are in the communication path, as in e-

Security. Applicant should amend the claim to clearly require what applicant regards as the invention.

9.   On pages 11-12, Applicant argues the rejection of claim 32. However, the arguments appear substantially similar to those presented with regard to claim 26, and thus are deemed not persuasive.

10.   On pages 12-13, Applicant argues the rejection of claim 33. However, the arguments appear substantially similar to those presented with regard to claim 26, and thus are deemed not persuasive.

11.   On pages 13-14, Applicant argues the rejection of claim 34. However, the arguments appear substantially similar to those presented with regard to claim 26, and thus are deemed not persuasive.

12.   On pages 14-15, Applicant argues the rejection of claim 35. More specifically, Applicant argues that "performing event correlation" is substantially different from "selecting a policy responsive to a common problem caused by an installation." However, in the proposed combination, the correlation of the events would lead to the selection of a policy for multiple network elements through the configuration plan.

13.   On page 16, Applicant argues the rejection of claim 36. More specifically,

Applicant argues that dynamic resource allocation is different from combining the

collection of security events. However, this argument is moot based on the new

grounds of rejection necessitated by the amendment.

14.   On page 17, Applicant agues the rejection of claim 37. However, this argument

is moot based on the new grounds of rejection necessitated by the amendment.

15.   On pages 17-18, Applicant argues the rejection of claim 38. However, the

argument appears substantially similar to that provided for claim 26, and is not

persuasive for substantially similar reasons.

16.   Applicants remaining arguments appear substantially similar to those presented

with respect to claims 26-38, and are not persuasive for similar reasons.

Claim Rejections - 35 USC § 103

17.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

18.   Claims 26-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Open e-Security Platform as in "Partner Sales Guide" from Winter 2002, hereafter

referred to as "e-Security" in view of Mattila et al. in US 2004/0049566, hereafter

referred to as "Mattila."

With regard to claim 26, e-Security discloses:

collecting real-time operation information on one or more first elements of a

network (e-Security: Page 13. As shown in the figure, e-Security agents are utilized to

collect information from disparate sources and correlate the information in a database.).

e-Security does not disclose expressly:

selecting a policy to be implemented by at least one second network element

different from the first network element, responsive to the collected real time information

from the one or more first network elements, the at least one second element including

an endpoint of the network and hosting an agent, and enforcing the selected policy on

the agent hosted by the at least one second network element.

However, Mattila discloses a system where a proxy (agent) is deployed onto a

network element and is used to perform the operations defined by a configuration plan

to change the settings of the network element (Mattila: Figure 2 and paragraph [0005]).

Thus, it would have been obvious to utilize the disclosure of Mattila in the method

of e-Security.

The suggestion/motivation for doing so would have been that e-Security is

concerned with the collection of information from disparate sources, including routers,

operating systems, firewalls, etc. (e-Security: Page 15). Thus, many of the detected

events will be unrelated to the cause of the problem. For example, information collected

from a firewall will typically show problems with other nodes on the network, not with the

firewall itself, as it usually reports on attempted intrusions. Thus, using a system such

as that of Mattila allows for agents to be utilized to perform the corrections required to

remedy the problems detected by the agents of e-Security.

With regard to claim 27, e-Security as modified by Mattila teaches that collecting

real-time operation information comprises collecting information on operation problems

(e-Security: Page 8. e-Security can view the status of different devices along with

logged information in the devices. Thus, the information may be related to operational

problems depending on the status of the devices.).

With regard to claim 28, e-Security as modified by Mattila teaches that collecting

real-time operation information comprises collecting information on software

applications installed or running on network elements (e-Security: Page 15. e-Security

collects data from operating systems, which includes software applications running on

network elements.).

With regard to claim 29, e-Security as modified by Mattila teaches the invention

as substantially claimed except that collecting real-time operation information comprises

collecting information on applications that do not operate or operate slowly.

However, Official Notice is taken that it was well known in the art to collect

information on system crashes.

Thus, it would have been obvious to collect information on system crashes in the

disclosure of e-Security as modified by Mattila.

The suggestion/motivation for doing so would have been that e-Security is

concerned with collecting information on security events. A crashed system may be

symptomatic of certain types of attacks that the network administrator should be made

aware of.

With regard to claim 30, e-Security as modified by Mattila disclsoes that

collecting information comprises collecting information on software applications installed

or running on the network elements (e-Security: Page 15. Information may be collected

on at least anti-virus software and operating systems.).

With regard to claim 31, e-Security as modified by Mattila teaches that collecting

real-time operation information comprises collecting information on the communications

between elements of the network (e-Security: Page 15. Included in the devices that are

monitored are intrusion detection, firewalls, and authentication, all of which include

information on some communication between elements on the network.).

With regard to claim 32, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting a policy relating to a software to be installed on the second network element.

However, official notice is taken that automatic updates of software were well known in the art.

Thus, it would have been obvious to have the configuration plan of -Security as modified by Mattila relating to software to be installed.

The suggestion/motivation for doing so would have been that often times merely changing the settings of a network element is not enough to correct a problem in a network, or to bring an element in line with the desires of a network administrator. Thus, having the configuration plan include information on where to fetch software and have instructions to install the software would allow e-Security as modified by Mattila to enjoy a higher level of automation.

With regard to claim 33, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting a policy relating to a software to be uninstalled from the second network element.

However, official notice is taken that automatic uninstalling software was well known in the art.

Thus, it would have been obvious to have the configuration plan of -Security as modified by Mattila relating to software to be uninstalled.

The suggestion/motivation for doing so would have been that often times merely changing the settings of a network element is not enough to correct a problem in a network, or to bring an element in line with the desires of a network administrator. Thus, having the configuration plan include information on where to fetch software and have instructions to uninstall the software would allow e-Security as modified by Mattila to enjoy a higher level of automation.

With regard to claim 34, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting a policy relating to preventing the installation of a software on the second network element.

However, it was well known in the art to prevent installation of software on network elements.

Accordingly, it would have been obvious to have the policy relate to preventing the installation of a software on the second network element.

The suggestion/motivation for doing so would have been that there would have been many reasons to prevent the installation of software. First, the software may have a known security vulnerability, thus making it undesirable to deploy the software on a large scale in a network. Further, virus and spyware scanners are concerned with preventing software to be installed, meaning that having the policy involve updating virus/spyware scanners would mean that the policy relates to preventing the installation of a software, where the software is a virus or spyware.

With regard to claim 35, e-Security as modified by Mattila teaches the invention as substantially claimed except that selecting the policy to be implemented comprises selecting responsive to a determination that a group of network elements having a common problem have installed thereon a specific software application or combination of software applications.

However, a person of ordinary skill in the art would have known how to perform this functionality.

Thus, it would have been obvious to have selecting the policy to be implemented comprises selecting responsive to a determination that a group of network elements having a common problem have installed thereon a specific software application or combination of software applications.

The suggestion/motivation for doing so would have been that e-Security is concerned with correlating events to allow connections between different events to be seen. Thus, if a combination of software applications is causing a problem, the information that was correlated could show this problem, and thus assist in determining the solution to the problem.

With regard to claim 36, e-Security as modified by Mattila teaches selecting a policy which allocates network resources (Mattila: Figure 2 and paragraph [0005]. The configuration plan of Mattila involves the allocation of network resources, as it configures the network devices.).

With regard to claim 37, e-Security as modified by Mattila teaches the invention

as substantially claimed except that the policy is implemented within less than 60

minutes from the collection of the information.

However, having the policy implemented within 60 minutes from the collection of

the information would have been well known to a person of ordinary skill in the art.

Thus, it would have been obvious to have the policy implemented within 60

minutes from the collection of the information.

The suggestion/motivation for doing so would have been that having a problem

resolved as quickly as possible allows the network to become error free as quickly as

possible, thus resulting in less potential loss. A person of ordinary skill in the art would

always be motivated to resolve issues as quickly as possible. Further, there is no

requirement as to how this implementation is to occur within 60 seconds that this

functionality is anything more than a responsiveness type guarantee.

With regard to claim 38, e-Security as modified by Mattila teaches that collecting

the operation information is performed repeatedly (e-Security: page 10. e-Security

provides real-time awareness, meaning that the information is collected in real-time).

With regard to claim 39, e-Security as modified by Mattila teaches that the

method is adapted to select the policy to be implemented by the at least one second

network element responsive to operation information collected from at least 2 first

network elements (e-Security: Page 15. Alerts are generated based on collected information from many network elements.).

With regard to claim 40, the disclosed invention is substantially similar that of claim 26, and is rejected for substantially similar reasons.

With regard to claim 41, e-Security as modified by Mattila teaches that the processor is adapted to find, for a group of network elements having a problem, a combination of attribute values that correlate with the problem to at least a predetermined degree (e-Security: Page 10, "Correlation." e-Security correlates events that may be related based on attributes of the event.).

With regard to claim 42, e-Security as modified by Mattila teaches the invention as substantially claimed except that the processor is adapted to find, for a group of network elements having a problem, a combination of attributes values that appears only on the network elements having the problem.

However, a person of ordinary skill in the art would have known how to have the processor is adapted to find, for a group of network elements having a problem, a combination of attributes values that appears only on the network elements having the problem.

Thus, it would have been obvious to have the processor is adapted to find, for a group of network elements having a problem, a combination of attributes values that appears only on the network elements having the problem.

The suggestion/motivation for doing so would have been that e-Security is intended to correlate events to find all the information that is relevant to a single event. Thus, finding a common attribute that is only on affected systems appears to be the intention of the correlation, which would allow connections to be found between the different elements.

With regard to claim 43, e-Security as modified by Mattila teaches that the processor is adapted to collect for at least one network element, a plurality of snapshot records of the network element at different times (e-Security: Page 13. The agents collect information in a continuous fashion from different event sources.).

With regard to claim 44, e-Security as modified by Mattila teaches that the processor is adapted to verify that each network element belongs to the network before collecting information from the network element (e-Security: page 13. There is no requirement as to what is meant by "belongs to the network." Being connected to a network constitutes "belong to the network." e-Security can only collect information from nodes that "belongs to the network." Therefore, if information is received, the node "belongs to the network.").

With regard to claim 45, e-Security as modified by Mattila teaches the invention as substantially claimed except that the processor is adapted to find groups using a k-clustering or hierarchy clustering method.

However, a person of ordinary skill in the art would have known how to have the processor of e-Security as modified by Mattila find groups using a k-clustering or hierarchy clustering method.

Thus, it would have been obvious to have processor of e-Security as modified by Mattila find groups using a k-clustering or hierarchy clustering method.

The suggestion/motivation for doing so would have been that both k-clustering and hierarchy clustering methods divide the network into smaller portions in order to facilitate different processes within the network. For example, k-clustering divides the network into non-overlapping sub networks, which then allows the monitoring and policy functions of e-Security as modified by Mattila to be performed with respect to the sub networks as far as collection and deployment, but correlated in a centralized fashion to allow the necessary correlation activities to be performed.

Conclusion

19.   **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time

policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Scott Christensen whose telephone number is (571)270-

1144. The examiner can normally be reached on Monday through Thursday 6:30AM -

4:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, William Vaughn can be reached on (571) 272-3922. The fax phone number

for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a

USPTO Customer Service Representative or access to the automated information

system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. C./
Examiner, Art Unit 2144

/William C. Vaughn, Jr./

Supervisory Patent Examiner, Art Unit 2444